Amendments to the Claims:

10

1. (Currently amended) A distributed system network for monitoring system a

communications network and for detecting an unauthorized communications access attempt

into the monitored communications network, the system comprising:

one or more distributed hierarchical monitoring systems; and

one or more alarm signals that represent an unauthorized communications access

attempt into one or more portions of the distributed monitored communications network,

wherein the one or more distributed hierarchical monitoring systems at least one of

analyze the unauthorized communications access attempt in response to the unauthorized

communications access attempt, and determine a responsive action to the unauthorized

communications access attempt, or forward information regarding the unauthorized access

attempt to one or more of the one or more hierarchical monitoring systems including sending

a mechanism for determining a source of the unauthorized communications access attempt in

a response to the unauthorized communications access attempt.

2. (Currently amended) The system of claim 1, further comprising a monitoring

device that monitors information on one or more distributed monitored communications

networks.

3. (Currently amended) The system of claim 1, further comprising an intrusion

analysis system that receives the one or more alarm signals and at least one of determines the

origin of the unauthorized communications access attempt, logs communications and

evaluates the threat of the unauthorized <u>communications</u> access attempt.

4. (Currently amended) The system of claim 1, further comprising an intrusion

interaction system that is capable of communicating with the origin of the unauthorized

communications access attempt.

5. (Currently amended) The system of claim 1, further comprising an escalation

determination system that, based on an evaluation of the unauthorized communications

W627968.1

access attempt and a comparison to one or more other unauthorized <u>communications</u> access attempts, forwards information regarding the unauthorized <u>communications</u> access attempt to the one or more of the one or more distributed hierarchical monitoring systems.

- 6. (Currently amended) The system of claim 1, wherein the one or more alarm signals is generated by one or more recipients of the unauthorized <u>communications</u> access attempt.
- 7. (Currently amended) The system of claim 1, further comprising a response system that communicates information <u>regarding the unauthorized communications access attempt</u> to one or more of a monitored site and a law enforcement agency.
- 8. (Currently amended) A method of protecting a distributed network for monitoring a communications network and for detecting an unauthorized communications access attempt into the monitored communications network, the method comprising:

monitoring one or more portions of the <u>distributed</u> <u>monitored communications</u> network through one or more <u>distributed</u> hierarchical monitoring systems; and

receiving one or more alarm signals that represent an unauthorized <u>communications</u> access attempt into one or more portions of the <u>distributed monitored communications</u> network,

wherein the one or more <u>distributed</u> hierarchical monitoring systems at least one of analyze the unauthorized <u>communications</u> access attempt <u>in response to the unauthorized communications access attempt</u>, <u>and</u> determine a responsive action to the unauthorized <u>communications</u> access attempt, or forward information regarding the unauthorized access attempt to one or more of the one or more hierarchical monitoring systems including sending a mechanism for determining a source of the unauthorized communications access attempt in a response to the unauthorized communications access attempt.

9. (Currently amended) The method of claim 8, further comprising monitoring information relating to on one or more geographic or organizational portions of the distributed network monitored communications networks.

1

10. (Currently amended) The method of claim 8, further comprising receiving the one

or more alarm signals and at least one of determining the origin of the unauthorized

communications access attempt, logging communications and evaluating the threat of the

unauthorized communications access attempt.

31

11. (Currently amended) The method of claim 10, wherein the logging can be

restricted based on an analysis of the unauthorized communications access attempt.

12. (Currently amended) The method of claim 8, further comprising communicating

with the origin of the unauthorized communications access attempt.

13. (Currently amended) The method of claim 8, further comprising forwarding,

based on an evaluation of the unauthorized communications access attempt and a comparison

to one or more other unauthorized communications access attempts, information regarding

the unauthorized communications access attempt to the one or more of the one or more

distributed hierarchical monitoring systems.

14. (Currently amended) The method of claim 8, wherein the one or more alarm

signals is generated by one or more recipients of the unauthorized communications access

attempt.

15. (Currently amended) The method of claim 8, further comprising communicating

information regarding the unauthorized communications access attempt to one or more of a

monitored site and a law enforcement agency.

16. (New) The system of claim 1, wherein the one or more distributed hierarchical

monitoring systems forward information regarding the unauthorized communications access

attempt to one or more of the one or more distributed hierarchical monitoring systems.

W627968.1

17. (New) The system of claim 1, wherein the determining mechanism includes an

identified packet concealed in the response, and the one or more distributed hierarchical

monitoring systems detect passage of the identified packet.

18. (New) The system of claim 17, wherein the packet is identified by a flag, and the

one or more distributed hierarchical monitoring systems detect passage of the flag.

19. (New) The system of claim 17, wherein the identified packet triggers reporting

showing a path to the source of the unauthorized communications access attempt.

20. (New) The system of claim 1, wherein the determining mechanism includes a

program concealed in the response.

21. (New) The system of claim 20, wherein the program is concealed in an HTML

page sent as part of the response.

22. (New) The method of claim 8, wherein the one or more distributed hierarchical

monitoring systems forward information regarding the unauthorized communications access

attempt to one or more of the one or more distributed hierarchical monitoring systems.

23. (New) The method of claim 8, wherein the determining mechanism includes an

identified packet concealed in the response, and the one or more distributed hierarchical

monitoring systems detect passage of the identified packet.

24. (New) The method of claim 23, wherein the packet is identified by a flag, and the

one or more distributed hierarchical monitoring systems detect passage of the flag.

25. (New) The method of claim 24, wherein the identified packet triggers reporting

showing a path to the source of the unauthorized communications access attempt.

W627968.1

- 26 (New) The method of claim 8, wherein the determining mechanism includes a program concealed in the response.
- 27. (New) The method of claim 26, wherein the program is concealed in an HTML page sent as part of the response.
- 28. (New) A computer program product including one or more computer-readable instructions configured to cause one or more computer processors to perform the steps recited in claim 8.
- 29. (New) The system of claim 2, wherein the monitored information relates to one or more geographic or organizational portions of the monitored communications networks.